

Previous SWR2310

Firmware version information

V2.04.04

New Functions

- Supports RADIUS servers.
- Supports SMTPS and SMTP authentication by the email notification function.
- Added the function to send a query when a topology change of spanning tree is detected by the IGMP/MLD snooping function.

Enhancements

- Expanded the number of slaves managed by L2MS from 64 to 128.
- Added the following information to the show stack command.
 - MAC address of Virtual switch
 - Serial number of Member switch
 - MAC address of Member switch
 - Link status of Stack port
- Supports the following for the configuration file control by TFTP.
 - Enables automatic restart when the startup config is updated.
 - Enables import and export of all settings of startup config.
- The following remote paths are used:
 - startup-config #0 All settings: config0-all
 - startup-config #1 All settings: config1-all
- The remote path for all the settings of Startup Config in the SD card is as follows.
 - startup-config #SD config.txt :configsd
 - startup-config #SD All settings: configsd-all
- Enables automatic adjustment of the vertical axis of the traffic information graph between 10 kbps and 10 Gbps on the dashboard of the Web GUI.
- Enables applying of the access list to the OUT direction of the VLAN interface in [Access List] in the detailed settings of Web GUI.

- Enables setting the tagged VLAN of the logical interface in [VLAN] of the detailed settings of Web GUI.

Fixed bugs

- Fixed the problem in which a memory leak would occur if the L2MS function was disabled in the state of LAN map warning detected during operating as an L2MS master.
- Fixed the problem in which restart was executed when a large number of SNMP packets were received.
- Fixed the problem in which communication may have been prevented when a slave switch with an IP address different from that of the master switch was connected by the stack function.
- Fixed the problem in which the ARP table was not updated in the Spanning Tree when a topology change had occurred and communication could have been temporarily disabled, depending on the configuration.
- Fixed the problem in which loop detection could not be performed when the switch whose stack ID was set to 2 was started in the stand-alone state, the stack was configured in the loop state, and then the stack was set to the stand-alone state again.
- Fixed the problem in which the following phenomenon occurred when stack ports were connected to form a stack while loops were detected:
 - The loop detection (shutdown) state of the slave switch was released in the stack function.
 - Congestion would occur despite the loop detection (blocking) state.
- Fixed the problem in which an incorrect snapshot warning log would be output to the slave switch in the stack function in case that the snapshot function was enabled when operating as an L2MS master during the stack configuration.
- Fixed the problem in which the following phenomenon may have occurred if the member switch was restarted in case that the 802.1X authentication was enabled on the logical interface during the stack configuration.
 - Web authentication could not be executed when Web authentication was combined on the concerned interface.
 - Could not communicate with terminals registered as static/forward on the concerned interface.
- Fixed the problem in which some frames addressed to MAC address could be flooded during the stack configuration.
- Fixed the problem in which MIB could not be acquired when a large number of SNMP packets were received during the stack configuration.

- Fixed the problem in which IPv4 link local address could not be set even if the stack was invalid on the stack compatible model.
- Fixed the problem in which the authentication screen might not be displayed if the supplicant is connected via a switch or wireless AP when Web authentication was enabled on the logical interface.
- Fixed the problem in which the automatic recovery setting of BPDU guard was invalid after rebooting in the spanning tree error detection function.
- Fixed the problem in which the IGMP/MLD snooping settings remained in the running config even if the VLAN was deleted.
- Fixed the problem in which entries of ARP table or IPv6 Neighbor table may have been illegally overwritten by the following operations when multiple static ARPs or static IPv6 Neighbors were registered to one VLAN.
 - VLAN interface was up
 - The ip/ipv6 forwarding command was run
- Fixed the problem in which the running config would not be applied correctly even if it was set by TFTP.
- Fixed the problem in which unnecessary error logs would be output when DHCP Offer was received from multiple DHCP servers.
- Fixed the problem in which packets with different port numbers would also meet the conditions even if a policy map including a port number specification was applied to an interface in QoS.
- Fixed some other minor bugs.